AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

Information associated with Rogreer32@gmail.com and homeimprovementbycl2014@gmail.com that is stored at premises controlled by Google LLC

Case No. 20-MJ-43

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

SEE ATTACHMENT A

over which the Court has jurisdiction pursuant to Title 18, United States Code, Sections 2703 and 2711, there is now concealed:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: Title 18 Sections 1956(a)(1), 1957(a), and 1343

The application is based on these facts: See attached affidavit.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days:_____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

S/A

Applicant's signature

IRS-CI Special Agent Matthew Rech III
Printed Name and Title

Sworn to before me and signed in my presence:

Date: 2/19/2020

Judge's signature

City and State: Milwaukee, Wisconsin

William E. Duffin, U.S. Magistrate Judge, U.S. Magistrate Judge
Printed Name and Title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Matthew Rech III, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises controlled by Google LLC ("Google"), an email provider headquartered at Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with Internal Revenue Service, Criminal Investigation (IRS-CI) and have been so employed since February 2006. My responsibilities as a Special Agent include the investigation of potential criminal violations of the Internal Revenue Code under Title 26 of the United States Code as well as related Title 18 and Title 31 offenses. In my career, I have conducted multiple investigations involving money laundering and have obtained seizure

warrants for criminal proceeds and property involved in money laundering and Title 31 offenses. In the course of those investigations, I have used various investigative techniques, including reviewing physical and electronic evidence, and obtaining and reviewing financial records. In the course of those investigations, I have also become familiar with techniques that criminals use to conceal the nature, source, location, and ownership of proceeds of crime and to avoid detection by law enforcement of their underlying acts and money laundering activities.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18 Sections 1956(a)(1) (money laundering), 1957(a) (unlawful monetary transactions), and Section 1343 (Wire Fraud), have been committed by those individuals and their accomplices discussed herein. There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United

States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. This investigation concerns a business email compromise ("BEC") scheme. A BEC scheme is a form of cybercrime that uses a fraudulent email to obtain funds from an organization or business entity. The scheme typically targets employees in financial roles and with access to entity funds within the victim organization. The fraudulent email will provide false instructions regarding financial transactions in order to defraud the employee into sending money or sensitive personal identifying data to the fraudster's bank account. Below are details relevant to the requested warrant.

7. Company 1, located in Texas, is a distributor of electrical and power generator parts. J.G. and K.R. are owners/partners of Company 1. Company 2 is an electrical and lighting contractor also headquartered in Texas. Company 2 purchases products from Company 1.

8. On June 24, 2019, a manager of Company 2 received an email purportedly from J.G. at Company 1 stating that Company 1 had recently made upgrades to their billing system, and that as of June 24, 2019, their bank account details changed for ACH/EFT payments. The email requested that Company 2 make the necessary changes to their billing system in order to avoid any delay in receiving payments from Company 1. The email included a letter with Company 1's letterhead and had ACH/EFT instructions listing Bank of America ("BOA") account

ending in # 6337, routing # 081904808, account name (Company 1), and remittance email of J.G.'s email address. Company 2's manager forwarded the new payment information to Company 2's corporate vender relations team, which processes ACH payments for Company 2's invoices.

9. On June 27, 2019, a separate email exchange occurred between a representative of Company 2 and K.R.'s email address (of Company 1) about when payment would be made on a recent invoice. The Company 2 representative wrote that the recent Company 1 invoice was entered into system and a payment check was cut. K.R.'s email address replied and requested that the Company 2's check be cancelled, and that Company 2 make payment according to the ACH/EFT instructions attached thereto, listing BOA account ending in # 6337, routing # 081904808, account name (Company 1), and the remittance email of J.G.'s email address. Thereafter, the Company 2 representative forwarded the information to Company 2's home office, which coordinates payments. The home office was able to cancel the check and began to process the payments according to the new instructions from Company 1.

10. On or about June 28, 2019, Company 2 initiated an ACH/EFT transfer of $527,398 from Company 2's bank account at BBVA Compass Bank to the BOA account ending in # 6337, routing # 081904808, specified in the new instructions from Company 1.

11. As discussed herein, the instructions from Company 1 to Company 2 regarding a new billing system were false and fraudulent.

12. Records from BOA for the account ending in #6337 show that the account was opened on September 17, 2018, in the name of Home Improvements by CL LLC, with the owner Corey Lee. The owner, Corey Lee, used his Wisconsin issued driver's license as identifying information when opening the account. No email address was associated with this account.

13. After the June 28, 2019, ACH/EFT transfer of $527,398 into the BOA account ending in #6337, there were several transactions:

a. On July 1, 2019, two BOA checks were purchased by Lee in the payee name of Home Improvements by CL LLC. One check was purchased at the BOA in Grayslake, IL, in the amount of $30,000, and the other was purchased at Waukegan Fountain Square BOA (IL) in the amount of $32,000. The two BOA cashier's checks for $30,000 and $32,000 were deposited on July 1, 2019, into US Bank account ending in # 9852, in the name of Home Improvements by CL LLC. Records associated with the US Bank account ending in #9852 show that the account was opened on June 21, 2018, in the name of Home Improvements by CL LLC, with the managing member Corey Lee.

b. On July 8, 2019, two US Bank cashier's checks were purchased by Lee with cash withdrawn from US Bank account ending in #9852, in the payee name of CARMAX and in the amounts of $20,102.67 and $20,000. These checks were endorsed and deposited by CARMAX in association with the July 9, 2019, purchase of a 2015 Mercedes Benz S550

by Lee. The vehicle had a total purchase price of $48,902.44. The remainder of the vehicle purchase was made with a debit card (US Bank #9852), cash, and a personal check for $4,390 from the US Bank account ending in #9852. The $4,390 personal check was returned NSF to CARMAX on July 16, 2019. Lee returned to CARMAX on July 17, 2019, to complete the purchase. He paid $4,000 cash and made a debit transaction for $405 from Educators Credit Union account ending #1697. The email associated with the purchase of this vehicle was clhomeimprovements@att.net

c. The BOA transactions of July 1, 2019, by Lee also included $32,500 in cash withdrawals; a cashier check for $100,090 in the payee name of Ace Telecom & Consultancy Services LLC; and a cashier check for $51,080 in the payee name of Vacant Times LLC. Both of these checks were purchased at the Waukegan Fountain Square BOA in Illinois.

d. The BOA transactions of July 1, 2019, by Lee also include a cashier's check in the amount of $19,476 to payee Rolando Greer. This check was deposited into Educators Credit Union savings member/account ending in #7757. A total of $19,550 was then transferred to checking member/account ending in #7757. A review of the checking and savings account records associated with account ending in #7757 show that the accounts were opened on November 6, 2013, with the sole member listed as Rolando R. Greer, who provided a Milwaukee address, a driver's license

as identification, and an associated email address of Rogrrer32@yahoo.com.

e. The BOA transactions on July 1, 2019, by Lee also include a wire transfer in the amount of $78,648 into the Educators Credit Union business checking member/account ending #4383S, and a cashier's check in the amount of $57,000 to payee All City Limousine Services, which was deposited into Educators Credit Union checking and savings member/account ending in #4383. A review of records associated with the checking and savings account ending in #4383 show that it was opened on April 27, 2017, in the name of All City Limousine Services LLC, with the sole member listed Rolando R. Greer. The email associated with this account was **rogreer32@gmail.com**. Throughout July 2019 a total of $55,275.88 was transferred from the business savings account ending in #4383 to the business checking account ending in #4383.

f. Throughout July 2019, a total of approximately $ $109,703.67 was transferred from the Educators Credit Union checking account ending in #4383 into Educators Credit Union checking member/account ending in #7757 belonging to Rolando R. Greer. An additional $1,200 was transferred from Educators Credit Union business savings account ending in #4383 into Educators Credit Union checking member/account ending in #7757. Throughout the month of July 2019, a total of approximately $83,128.31 in cash/ACH withdrawals was made from the Educators Credit

Union account ending in #7757, including a $27,400 cash withdrawal for an Educators Credit Union cashier's check dated July 3, 2019, in the full amount $27,400 to payee Lux Cars, with a remitter of Roland R. Greer.

g. The Educators Credit Union cashier's check for $27,400 was cashed and deposited by Lux Cars of Chicago, in connection with the July 3, 2019, purchase of a 2013 Mercedes B S550 Sedan for a total of $27,488.

h. Two personal checks from Educators Credit Union account ending in #7757 were also cleared in July 2019. These checks were made out to Home Improvements by CL LLC (Check #1177 in the amount of $9,800 and Check #1178 in the amount of $10,200). These two personal checks were deposited in into Educators Credit Union account ending in #1697. A review of records associated with the account ending in #1697 showed that the account was opened March 21, 2019, in the name of Home Improvements by CL LLC, with Corey Lee identified as CEO of the business and only responsible member for the account. The email address associated with opening this account was clhomeimprovements@att.net.

i. On July 10, 2019, an additional $7,000 cash deposit was made into the Educators Credit Union account ending in #1697. During the month of July 2019, a total of approximately $24,141 in debit/ATM withdrawals were conducted on this account. Included in these debits were airline charges and various debit transactions in Miami, Florida.

14. A few days after processing the ACH transfer to BOA, an official from BOA contacted Company 2 about the $527,398 transfer to one of their customers. A Company 2 representative confirmed to BOA that the customer BOA identified as the receiver of the funds was not the intended receiver of the ACH transfer.

15. The Company 2 representative then reached out to BBVA bank where the $527,398 ACH transfer originated. BBVA confirmed the receipt of the ACH by BOA and then attempted to recall the funds from BOA. The BOA account ending in #6337 was closed on August 12, 2019, and the remainder of $124,900.35 was sent back to Company 2's BBVA bank account.

16. As part of the investigation, the owners/partners of Company 1 were contacted and they confirmed the following:

a. On July 9, 2019, Company 1 contacted Microsoft 365 Data Protection Support Engineer Department, which confirmed that the two email accounts of Company 1's owners/partners had been compromised by use of a filter setup. The Company 1 email addresses were "hacked" to delete various legitimate emails from the Company 1 owners/partners, and then the hackers would send out and receive emails using the actual Company 1 partners' email addresses.

b. No one had permission to use the Company 1 name and logo to misrepresent their company and change the payment method on outstanding invoices to the BOA account ending in #6337.

c. Email communications of the Company 1 owners/partners and various vendors were compromised between the approximate dates of June 24, 2019, and July 8, 2019.

17. As part of the investigation, investigators obtained the Internet Protocol "IP" address used to log into the BOA bank accounts remotely. The IP addresses used to log into the BOA "Home Improvements by CL LLC" account ending #6337 were 104.231.219.66 and 75.86.9.112. Subscriber information associated with these IP addresses shows that IP address 104.231.219.66 was listed from May 1, 2019, until September 19, 2019, to Corey Lee, located at XXXX N. 51st Blvd., Milwaukee, WI 53216, and email address homeimproveimprovementbycl2014@gmail.com. IP address 75.86.9.112 was listed from March 5, 2018, to August 1, 2019, to Rolando Greer with an address of XXXX N. 40th St., Milwaukee, WI 53216, and email address **Rogreer32@gmail.com**.

18. Subscriber information from Google for email account **Rogreer32@gmail.com** shows that the account was created on January 3, 2010, and lists the subscriber's name as Rolando Greer. The account lists a recovery email of Rogreer1971gl@yahoo.com.

19. Subscriber information from Google for email accounts homeimproveimprovementbycl2014@gmail.com and **homeimprovementbycl2014@gmail.com** was obtained as part of the investigation. Information from both accounts was requested in case the information provided by the Internet Service Provider (noted above) was entered incorrectly. The subscriber

information for homeimprovementbycl2014@gmail.com shows that it was listed with the name Corey Lee, and has recovery email clhomeimprovements@att.net.

20. Subscriber information from Oath Inc., for email account clhomeimprovements@att.net shows that it was created on February 21, 2010, and lists the subscriber's name as Corey Lee.

21. Based on my training and experience, and information provided by other members of law enforcement, I know that oftentimes, individuals engaged in BEC schemes target multiple victims in order to maximize gains. Further, individuals engaged in these schemes take time to prepare the scheme, including communicating with associates, creating bank accounts, and related matters, as well as collect information about targeted victims. This process can take weeks, months or years depending on the scope of the scheme.

22. As part of this investigation, I obtained evidence indicating that Corey Lee and Rolando Greer have been involved in other fraud schemes.

a. As part of federal law enforcement de-confliction, it was revealed that in early March 2018, the FBI interviewed complainant G.F., the owner of a large business located in Florida. G.F.'s bookkeeper had been the target of an email scheme wherein someone took control of the email and directed three separate transfers from G.F.'s Bank of America account into various unknown actor's accounts. The investigation determined that one of these unauthorized transfers took place on March 7, 2019, in which a deposit of $450,000 was transferred from the BOA account into a Wells

Fargo checking account ending in #2226. This account was titled to All City Limousine Services LLC with Rolando Greer as the sole owner and signer of account. Greer opened this account on November 10, 2018, and listed a business address in Milwaukee, WI, and an email address of **rogreer32@gmail.com**. After this deposit, numerous personal checks were written out and cashed to Greer, Lee, and other individuals. Greer also purchased two cashier checks and made a payment to his Capitol One Credit Card.

b. Further, as part of this investigation, I also communicated with representatives of two other companies, L.L. and A.L., A.L. provides financial services to customers on behalf of clients who enlist their services. In the process of attempting to provide payment on behalf of their customer to L.L., A.L. contacted a representative L.L. on or around October 3, 2018, and invited L.L. to sign up to the payables system. On or around October 9, 2018, a payment of $102,095.22 was deposited into a US Bank account ending in #9852. This account was titled to Corey Lee DBA Home Improvement by CL LLC. Lee opened this account on June 21, 2018, and listed an address in Milwaukee, WI. Shortly aftert this transaction, L.L. notified A.L. that on or around the time of the $102,095.22 transaction, their computer systems were hacked and an imposter had actually registered for the payment with A.L. and entered a

banking account not owned or authorized by L.L. to receive payments on their behalf.

c. As part of the investigation, I reviewed an complained sent to the FBI Internet Criminal Complaint Center stating that an individual named K.T. was a victim of a BEC scheme. The report stated K.T. and a colleague received an email containing fraudulent wire instructions for a transfer from First Republic Bank to Wells Fargo in the amount of $200,000 on May 8, 2018. A review of banking records determined that the $200,000 was deposited into Wells Fargo Checking Account ending in #6277. This account was titled to Home Improvement by CL LLC and had Corey Lee listed as the sole owner and signer of account. Lee opened this account on April 18, 2019, and listed an address in Milwaukee, WI, and an email address of clhomeimprovements@att.net.

23. In general, an email that is sent to a Google subscriber is stored in the subscriber's "mail box" on Google servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Google servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google servers for a certain period of time.

BACKGROUND CONCERNING EMAIL

24. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail ("email") access, to the public. Google allows subscribers to obtain email accounts at the domain name gmail.com

like the email accounts listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

25. A Google subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

26. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to

identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

27. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

28. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute

evidence of the crimes under investigation because the information can be used to identify the account's user or users.

29. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location

information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

30. Based on the forgoing, I request that the Court issue the proposed search warrant.

31. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Rogreer32@gmail.com and homeimprovementbycl2014@gmail.com that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at Mountain View, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account January 1, 2018, to the present, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within 10 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 18 Sections 1956(a)(1) (money laundering),1957(a) (unlawful monetary transactions), and Section 1343 (wire fraud), those violations involving Corey Lee, Rolando Greer, or their accomplices or associates, and occurring after January 1, 2018, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Business email compromise schemes, including efforts to prepare for conceal the scheme, or the identities of any person involved in such a scheme;

(b) Communications relating to Company 1, Company 2, G.F., K.T., A.L., L.L., their representatives, businesses, employees, employers, associates, or affiliates;

(c) Financial transactions, financial instruments, communications concerning financial transactions, financial institutions, or acts involving or potentially involving stolen moneys;

(d) Establishing, operating, or ending business entities;

(e) Compromising computers, computer systems, or email accounts;

(f) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account

access, use, and events relating to the crime under investigation and to the email account owner;

(g) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(h) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

(i) The identity of the person(s) who communicated with the user ID about matters relating wire fraud, money laundering, or unlawful financial transactions, including records that help reveal their whereabouts.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google LLC, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google LLC. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google LLC, and they were made by Google LLC as a regular practice; and

b. such records were generated by Google LLC's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google LLC in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Google LLC, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date	Signature